The Centre for
Social Anthropology
and Computing

University of
Kent

School of Anthropology
and Conservation
Marlowe Building
Canterbury CT2 7NR

Tel: +44 1227 823144
Fax: +44 1227 827289
m.d.fischer@kent.ac.uk

Saturday, 1 June 2013

Sally A. Applin - [redacted]
Prof. Michael D. Fischer - m.d.fischer@kent.ac.uk

Ms. Karen Jagielski, Bureau of Consumer Protection
Mr. Jay Mayfield, Office of Public Affairs
Federal Trade Commission

Re: Input to FTC on Privacy and Security Implications of the IOT

Dear Ms. Jagielski, Mr. Mayfield and FTC/IoT Investigative Staff,

Please find attached our input on the privacy and security implications of the IoT.
Although we are affiliated with UKC, as US citizens and social scientists, we have a great concern for the safety and health of the public citizenry as we all adapt to new technologies.

Please let us know if we may provide any further details to the attached considerations.

Kind regards,

[Signed]

Sally Applin
Prof. Michael D. Fischer

Privacy and Security issues relating to IoT

1) ***Credentials***: The IoT will result in a situation where private devices will interact with their owners, or more pointedly, with people (or machines) exercising the credentials of their owners. This will be a requirement of these systems under a full IoT vision, as many relationships will not be one to one with individuals, but there will be managerial devices as well that will require these credentials.

Thus, one requirement is a reasonable system of establishing, verifying and protecting credentials. Although some advocate biometric based credentials, such as finger prints or retinal scans, this is a highly dangerous option since in dealing with only pieces of a person, it may encourage the hijacking of body parts to gain access to people's homes and possessions, online financial resources etc. An alternative would be to develop biometric indices comprised of a number of systemic readings from the body which at least requires the hijacking of complete and normally functioning bodies. This would be developed as parameters into some kind of large primes algorithm that is similar to trap-door functions used for current encryption. The goal being that the algorithm would be unable to decompose into information other than determining that the current biometric was different from another one.

2) ***Public Safety***: Safe ways for people to constantly interact with their devices will need to be in place. The evidence suggests that people will respond and interact with their devices just as they do with other people, a job that is increasingly difficult to manage. We already see this in people fiddling with their phones or GPS systems in the car, or even on street intersections as pedestrians. We have seen the rise in "Apple picking" type crimes of "grab and go" theft of handheld devices in urban areas. With the IoT, there will be more ubiquitous interaction requiring even more overt device usage in public and thus, more safety and security.

3) ***External Management***: Because of the requirements of satisfying 1) and 2) above, it is likely that people will require small to large commercial firms to assist in seamlessly managing their lives; there is simply too much logic and communications for individual people to manage on their own. These firms will need careful oversight, as effectively any employee able to compromise a client's account will have control over much of that individual's property in terms of access and acquisition.

4) ***Public Commons Impact***: In addition to private devices, there will be public devices that will be an integrated part of the overall life system, and people will want and need to connect to these. These would include the mundane, such as vending machines, public safety, such as traffic management apparatus, and local information nodes. But there is a likelihood that without regulation, serious social divisions could emerge. For example, stores that check credit balances prior to permitting entry, and eventually whole areas that are only open to 'members' or individuals with specific profiles. This could seriously imbalance the current balance of public and private space, and in particular public access to private space.

5) ***Surveillance***: Surveillance by private citizens, firms, corporations and government bodies will be greatly simplified with the IoT, and in combination with data mining will make it possible to virtually strip away any semblance of privacy. Currently there are tools available to concerned individuals that make it possible to be online more or less invisibly, but this requires awareness and skill. For example, through a combination of anonymous proxies, Tor, VPNs, VPS it is possible to casually guard one's privacy. There is no reason that a regulated public utility could not be created that would perform much of the same function. This would contribute to solving many of the problems above, since any tokens of identity sent over the network would be explicitly under the control of the client, and could be selectively used or withheld. Spatial tracking would be impossible without consent.

6) ***Privacy***: It is essential that individuals be in control of when they can and can not be tracked and when their identity is proffered. If it is the latter, then the identity should be proffered through an 'identity proxy' that delivers a partial identity (from a profile that is created and verified) to different kinds of concerns via the public utility which has to be trusted. In this way, people will have partial and untraceable identities except for the instances when they need and require a full and unique one.

Background

As social and behavioral scientists, a chief concern with the IoT is how populations will adapt and respond to the IoT and how these changes in behavior will impact social patterns. With the mobile web most people under 50 want (and use) a nearly continuous connection to maintain relationships and exchange information throughout the day. The desire to connect often impairs sound judgement, diverting attention from more immediate responses to local events. People text and talk while driving, which leads to injury and fatalities, and they continue to do so, even when laws are put in place.

If we have a population already overwhelmed from talking, messaging and managing their human relationships, adding more relationships with machines generating messages that stimulate response, reply or action, will become even more overwhelming. Thus, we are concerned that adding the management of more messages to an already overwhelmingly large cache of obligations will create incentives for the development of infrastructure changes that will serious impact citizen privacy and safety unless contained.

The question then becomes how to use artificial intelligence as an underpinning architecture to offload the need for people to respond to every and each single message, and do this in a manner which does not compromise individual privacy and security.